UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,430	12/31/2003	HongQian Karen Lu	76.0888	1787

41754 7590 11/20/2007

THE JANSSON FIRM
9501 N. CAPITAL OF TX HWY #202
AUSTIN, TX 78759

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
11/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/750,430	LU ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending in this office action.

2. Applicant's arguments, filed September 17, 2007, have been fully considered but are moot in view of the new grounds of rejection.

Specification

3. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-15 and 17-19 are rejected under 35 U.S.C. 102(a/e) as being anticipated by Asunmaa et al. (U.S. Patent Pub. No. 2003/0172090).

Regarding claim 1, Asunmaa et al. teaches a method for effecting secure transactions over a computer network **that includes an untrusted client computer with a user interface and a server computer** (fig. 1, ref. num 110-130, and 160), in a manner designed to foil identity theft perpetrated from **the client** computer, comprising:

- Connecting a secure computing device to the network (fig. 1, ref. num 140);
- Operating the secure computing device to communicate a list of available services, **for which the secure computing device stores private information corresponding to the device,** to the client computer (fig. 3, ref. num 313 and paragraph 0174);
- Responsive to receiving the list of available services using the user interface to display the list of available services to a user (paragraph 0109);
- Responsive to a selection of one available service by the user, establishing a secure connection from the secure computing device to the server (fig. 1, ref. num 165);
- Securely communicating private information from the secure computing device to the server over the secure connection (paragraph 0169).

Regarding claim 2, Asunmaa et al. teaches further comprising:

- Authenticating a user based on the private information (paragraph 0173); and
- In response to successful authentication of the user, conducting a transaction between the client computer and the server computer (paragraph 0175).

Regarding claim 3, Asunmaa et al. teaches further comprising transmitting from the secure computing device to the server computer user identifying information (paragraph 0169).

Regarding claim 4, Asunmaa et al. teaches wherein the user identifying information includes a secret personal identification number (sPIN) (paragraph 0190).

Regarding claim 5, Asunmaa et al. teaches further comprising responsive to receiving the user identifying information, operating the server computer to establish an association among the user, the client and the secure computing device (fig. 5 and paragraph 0172).

Regarding claim 6, Asunmaa et al. teaches wherein the secure computing device has a personal identification number (PIN) wherein the sPIN and the PIN are unrelated (paragraph 0080 and paragraph 0190).

Regarding claim 7, Asunmaa et al. teaches wherein the server computer uses the sPIN for only one session (paragraph 0190).

Regarding claim 8, Asunmaa et al. teaches wherein the portable secure computing device is a smart card (paragraph 0100).

Regarding claim 9, Asunmaa et al. teaches a method for secure transactions over a computer network **that includes an untrusted client computer with a user interface and a server computer** (fig. 1, ref. num 110-130 and 160), in a manner designed to foil identity theft perpetrated from **the client** computer, comprising:

- Connecting a secure computing device to the network (fig. 1, ref. num 140);
- Establishing a secure connection from the secure computing device to the server (fig. 1, ref. num 165);
- Securely communicating private information from the secure computing device to the server over the secure connection (paragraph 0169);
- Authenticating a user using the private information (paragraph 0173); and
- In response to successfully authenticating the user, conducting a transaction between the client and the server (paragraph 0175).

Regarding claim 10, Asunmaa et al. teaches wherein the step of securely communicating private information comprises pushing the private information from the secure computing device to the server computer (paragraph 0181).

Regarding claim 11, Asunmaa et al. teaches further comprising in response to successfully authenticating a user, operating the client to transmit an indication to the server that the secure computing device will send information necessary for a transaction; operating the server to wait for the information from the secure computing device; operating the client to select the information necessary for the transaction; and in response to selecting the information necessary for the transaction, operating the secure computing device to transmit the selected information securely to the server (paragraph 0153-0155).

Regarding claim 12, Asunmaa et al. teaches wherein the step of securely communicating private information comprises operating the server computer to pull the private information from the secure computing device (paragraph 0181).

Regarding claim 13, Asunmaa et al. teaches further comprising in response to successfully authenticating a user, operating the server to transmit a request to the secure computing device to provide information necessary to complete a transaction; in response to a request from the server for information necessary to complete a transaction, operating the secure computing device to notify the client that the server has made the request for information necessary to complete a transaction; in response to notification from the secure computing device that the server is requesting the information necessary to complete a transaction, operating the client to obtain a user's approval or denial of the request; and in response to a user's approval, transmitting the

requested information from the secure computing device to the server in a secure manner (fig. 5 and paragraph 0172).

Regarding claim 14, Asunmaa et al. teaches a system for effecting secure transactions over a computer network **that includes an untrusted client computer with a use interface and a server computer** (fig. 1, ref. num 110-130 and 160), in a manner designed to foil identity theft through keystroke logging, comprising:

- A secure computing device connected to the computer network and capable of establishing a secure connection with the server computer and the client computer (fig. 1, ref. num 140 and fig. 1, ref. num 165);
- Wherein the secure computing device has logic operable to store private user information (fig. 3, ref. num 313); and
- Wherein the secure computing device has logic, in response to the initiation of a transaction between a user operating the client computer and the server computer, operable to securely transmit the private user information to the server computer in a manner such that only the server can interpret the private user information (paragraph 0169).

Regarding claim 15, Asunmaa et al. teaches wherein the secure computing device has logic to transmit a map to the server computer, the map having the elements clientIP, cardIP, login credentials, and secret personal identification number (sPIN) (paragraph 0138); wherein the server computer has logic to request **the** user to enter

the sPIN and logic to verify that the entered sPIN matches the sPIN in the map (paragraph 0109).

Regarding claim 17, Asunmaa et al. teaches wherein the secure computing device transmits the private user information upon a request by the user (paragraph 0198).

Regarding claim 18, Asunmaa et al. teaches wherein the secure computing device transmits the private user information upon a request by the server computer (paragraph 0199).

Regarding claim 19, Asunmaa et al. teaches wherein the secure computing device transmits the private user information to the server computer only upon permission granted by the user (paragraph 0199).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 16 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asunmaa et al. (U.S. Patent Pub. No. 2003/0172090) in view of Blatherwick et al. (U.S. Patent No. 6,269,395).

Regarding claims 16 and 20, Asunmaa et al. does not teach destroying a map if the sPIN's do not match.

Blatherwick et al. teaches destroying the maps if the sPINS's do not match (fig. 14.2.2.1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine destroying maps if the sPIN's do not match, as taught by Blatherwick et al., with the system of Asunmaa et al. It would have been obvious for such modifications because the sPIN is a session secret; once it is determined that the sPIN's do not match, deleting the data is the most secure way of preventing replay attacks.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/19/07